PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-215119
(43)Date of publication of application : 06.08.1999

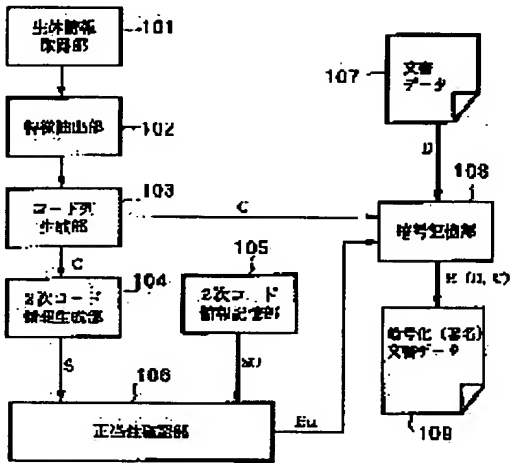
(51)Int.Cl. H04L 9/32
A61B 5/117
G06T 7/00
G09C 1/00
G09C 1/00
G09C 1/00

(21)Application number : 10-011764
(22)Date of filing : 23.01.1998

(71)Applicant : CANON INC
(72)Inventor : OTA KENICHI

(54) DEVICE AND METHOD FOR MANAGING PERSONAL INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To improve the reliability of an electronic signature of a person using his secret key and, at the same time, to prevent the risk that the secret key is illegally used by another person.
SOLUTION: A feature extracting section 102 extracts the biological feature of a person from the biological information (for example, pictures taken with a fundus camera) of the person acquired by a biological information acquiring section 101 while a code train generating section 103 generates a code train C by digitizing the extracted biological feature. A secondary code information generating section 104 generates secondary code information S based on the code train C. A correctness confirming section 106 compares the secondary code information with preregistered secondary code information S0 and, when the section 106 confirms that the code train C is acquired from the specific personal, an enciphering section 108 generates signature data 109 by enciphering document data by using the above-mentioned code train C.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] Personal-information-management equipment characterized by providing the following. An extract means to extract the individual living body feature A coding means which carries out the digital coding of the living body feature extracted with said extract means Secondary code generation means to generate secondary code information based on a digital code coded with said coding means A check means to check the justification of secondary code information generated with said generation means, and a signature data generation means to generate signature data based on the living body feature coded with said coding means when justification was checked with said check means
[Claim 2] Said signature data generation means is personal-information-management equipment according to claim 1 characterized by making an extract of the living body feature of an individual by said extract means, and digital coding processing of the living body feature by said coding means redo when justification is not checked with said check means.
[Claim 3] Said signature data generation means is personal-information-management equipment given in either claim 1 characterized by enciphering processing-object data based on the living body feature coded with said coding means, and using encryption data as signature data, or claim 2.
[Claim 4] A manuscript image characterized by providing the following is read, and it includes in a manuscript image copy system which has a manuscript image reading means in which an output is possible as a manuscript picture signal, and an output means to output a manuscript picture signal read with said manuscript image reading means as a corresponding visible image, and is possible personal-information-management equipment. An extract means to extract the individual living body feature A coding means which carries out the digital coding of the living body feature extracted with said extract means Secondary code generation means to generate secondary code information based on a digital code coded with said coding means An encryption means encipher the manuscript picture signal read with said manuscript image reading means based on the living body feature coded with said coding means when justification is checked with a check means check the justification of secondary code information generated with said generation means, and said check means, and a conversion means change into visible image data the signal enciphered with said encryption means, and output to said output means
[Claim 5] Said secondary code information is personal-information-management equipment according to claim 1 to 4 characterized by being the predetermined thing changed and generated with a tropism function on the other hand about a code train which carried out the digital coding of the living body feature.
[Claim 6] The justification of said secondary code information is personal-information-management equipment according to claim 1 to 5 characterized by being checked by comparison with secondary code information registered beforehand and secondary code information generated with said secondary code generation means.
[Claim 7] The individual humanity news management method which carries out the digital coding of the living body feature which extracted and extracted the individual living body feature, and is characterized by the thing which generate signature data based on said coded living body feature

when the justification of secondary code information which generated and generated secondary code information based on said coded digital code checks and justification is checked, and do for signature data generation.
[Claim 8] An individual humanity news management method according to claim 7 characterized by making an extract of said individual's living body feature, and digital coding processing of said living body feature redo when the justification of said secondary code information is not checked.

[Claim 9] Generation of said signature data is an individual humanity news management method given in either claim 7 characterized by being what enciphers processing-object data based on the living body feature coded with said coding means, and uses encryption data as signature data, or claim 8.
[Claim 10] A manuscript image is read and it is the manuscript image reading means in which an output is possible as a manuscript picture signal. An output means to output a manuscript picture signal read with said manuscript image reading means as a corresponding visible image The digital coding of the living body feature which is the individual humanity news management method equipped with the above, and was extracted by extracting the individual living body feature is carried out. The justification of secondary code information generated by generating secondary code information based on said coded digital code is checked. It is characterized by changing a signal which enciphered a manuscript picture signal read with said manuscript image reading means based on said coded living body feature when justification was checked, and was enciphered further into visible image data, and outputting to said output means.
[Claim 11] Said secondary code information is personal-information-management equipment according to claim 7 to 10 characterized by being the predetermined thing changed and generated with a tropism function on the other hand about a code train which carried out the digital coding of the living body feature.
[Claim 12] The justification of said secondary code information is an individual humanity news management method according to claim 7 to 11 characterized by being checked by comparison with secondary code information registered beforehand and secondary code information generated with said secondary code generation means.
[Claim 13] A computer-readable record medium characterized by coming to record a control procedure which realizes a function according to claim 1 to 12.
[Claim 14] A computer program train characterized by realizing a function according to claim 1 to 12.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[The technical field to which invention belongs] This invention manages individual humanity news based on the individual living body-feature, for example, relates individual signature information and a manuscript copy to controllable personal-information-management equipment and a controllable method based on the individual living body-feature.
[0002]
[Description of the Prior Art] Current and a network system develop and many technology of the electronic banking and cybermoney on a network is examined. When an individual is going to trade electronically using this network system, the individual who is demanding dealings must be correctly discriminated from a remote place. For this reason, the electronic signature technology using the so-called unsymmetrical public key systems, such as a RSA method, is examined.
[0003] An unsymmetrical public key system sets up the key information on the pair a "public key" and a "private key", and when the document which an individual publishes using the private key which the individual has is signed, if not based on the same people's public key, it has the feature that the document is undecipherable. Then, if an individual (referred to as Mr. A) manages a private key so that it may not be known by others by any means, he enciphers the order document of dealings of Mr. A with the private key and transmits to a dealings partner (referred to as Mr. B), it can check that the publisher of an order sheet is Mr. A rightly since the document can decode Mr. B only with Mr. A's public key.
[0004] The identification equipment which compares the eyegrounds image of the past which memorized the video signal which used solid state image sensors, such as Area CCD, carried out electronic photography of the eyegrounds image, and, on the other hand, carried out the electronic image pick-up with ophthalmology equipments, such as a fundus camera, in order to attest a specific individual to accuracy more to storages, such as a hard disk, and was memorized by this storage with the current eyegrounds image by which electronic photography was newly carried out, and identified the individual is known.
[0005]
[Problem(s) to be Solved by the Invention] However, there were the following troubles in the encryption system of the above-mentioned conventional example. That is, although it is necessary to set up the password called a private key in the electronic signature technology using a general unsymmetrical public key system which was mentioned above in order to identify an individual, it must be made a password to some extent complicated in order to prevent surreptitious use of the key by others, for considering as a positive thing, the digit count etc. must be made [many], the limit which an individual can memorize is crossed, and there is a problem of not being practical.
[0006] Although the method of making it memorize on a certain storage rather than memorizing this password individually, and saving it is also considered, there is no guarantee that reading appearance of that storage is not done by the others, and it has a problem in the viewpoint of safety. Moreover, the information for specifying an individual, when saying that personal authentication will be carried out using an eyegrounds image, i.e., the image information which

carried out electronic photography of the individual eyegrounds image, had to be beforehand memorized to storage, and there was a problem that reliable personal authentication will become impossible when this storage information has been plagiarized.
[0007] As mentioned above, an effective method which solves the problem of the personal authentication in electronic dealings was not proposed.
[0008]
[Means for Solving the Problem] This invention was made for the purpose of solving a technical problem mentioned above, and is equipped with the following configurations as a way stage which attains this purpose. Namely, an extract means to extract the individual living body feature and a coding means which carries out the digital coding of the living body feature extracted with said extract means, Secondary code generation means to generate secondary code information based on a digital code coded with said coding means, It is characterized by having a check means to check the justification of secondary code information generated with said generation means, and a signature data generation means to generate signature data based on the living body feature coded with said coding means when justification was checked with said check means.
[0009] And for example, said signature data generation means is characterized by making an extract of the living body feature of an individual by said extract means, and digital coding processing of the living body feature by said coding means redo, when justification is not checked with said check means. Moreover, for example, said signature data generation means is characterized by enciphering processing-object data based on the living body feature coded with said coding means, and using encryption data as signature data.
[0010] A manuscript image is read. Or a manuscript image reading means in which an output is possible as a manuscript picture signal, An extract means to be personal-information-management equipment in which inclusion to a manuscript image copy system which has an output means to output a manuscript picture signal read with said manuscript image reading means as a corresponding visible image is possible, and to extract the individual living body feature, A coding means which carries out the digital coding of the living body feature extracted with said extract means, Secondary code generation means to generate secondary code information based on a digital code coded with said coding means, A check means to check the justification of secondary code information generated with said generation means, An encryption means to encipher a manuscript picture signal read with said manuscript image reading means based on the living body feature coded with said coding means when justification is checked with said check means, It is characterized by having a conversion means to change into visible image data a signal enciphered with said encryption means, and to output to said output means.
[0011] And for example, it is characterized by said secondary code information being predetermined things changed and generated with a tropism function on the other hand about a code train which carried out the digital coding of the living body feature. Moreover, for example, justification of said secondary code information is characterized by being checked by comparison with secondary code information registered beforehand and secondary code information generated with said secondary code generation means. Moreover, the digital coding of the living body feature which extracted and extracted the individual living body feature carries out, and when the justification of secondary code information which generated and generated secondary code information based on said coded digital code checks and justification is checked, it is characterized by to have a means which carries out signature data generation generate signature data based on said coded living body feature.
[0012]
[Embodiment of the Invention] Hereafter, the example of a gestalt of implementation of 1 invention which relates to this invention using a drawing is explained to details.
The example of a gestalt of implementation of the first invention concerning this invention is explained below [the example of a gestalt of the first operation]. The example of a gestalt of implementation of the first invention explains supposing the case where a certain individual (referred to as Mr. A) performs the electronic signature of the example of a gestalt of this operation to the target document data using unsymmetrical public key cryptosystems, such as a RSA method.

[0013] Usually, in the unsymmetrical public key cryptosystem, Mr. A owns the "private key" and the "public key" as two cryptographic keys. Although all are expressed by the dozens of bits to hundreds of bits bit string and only Mr. A knows a "private key", generally the "public key" is exhibited. Now, when Mr. A enciphers a certain document using his own "private key", the enciphered document cannot be decoded if not based on Mr. A's public key.
[0014] since the Mr. A's "private key" was not known other than Mr. [A], the document was enciphered by Mr. A that a certain document can decode with Mr. A's "public key" -- namely, Mr. A -- it is decided that it is the document with which he signed. however, the above -- setting -- "a private key" -- him -- the individual memorizes, or a storage must be made to memorize as a certain digital data, and the safety is not enough as the conventional example explained although this needed to be kept severely since not being known except was a premise.
[0015] In the example of a gestalt of this operation, the safety of a "private key" can be guaranteed by using the configuration of drawing 1 . Drawing 1 is the block diagram showing the configuration of the personal-information-management equipment in the example of a gestalt of implementation of the first invention concerning this invention. In drawing 1 , 101 is the biological information acquisition section and acquires biological information of the individual (here Mr. A) who owns the private key. For example, in order to identify the specific individual of being as acquiring a fingerprint pattern image two-dimensional **** [, and], the living body-information said to be effective is acquired by the well-known method. [picturizing the vasa-sanguinea-retinae pattern of eyegrounds with the fundus camera using a CCD image sensor]
[0016] 102 is the feature-extraction section and the feature-extraction section 102 performs a feature extraction from the biological information obtained in the biological information acquisition section 101. For example, a thing as shown in JP,7-213511,A ("identification equipment") as a method of extracting characteristic quantity from the blood vessel pattern of eyegrounds can be used. This detects a mammary-papilla center position from an eyegrounds image, and detects the angle component of the location where an eyegrounds image is scanned in the shape of a concentric circle from the center position, and a blood vessel exists.
[0017] 103 is the code train generation section and generates a predetermined code train based on the angle component obtained from the feature of the biological information extracted in the feature-extraction section 102. For example, although it has detected whether you are him in JP,7-213511,A mentioned above as compared with the reference pattern of the specific individual who has saved the detected angle component beforehand, the code train generation section 103 generates a predetermined code train based on the obtained angle component in the example of a gestalt of this operation.
[0018] The situation of the code train generation by the code train generation section 103 is shown in drawing 2 and drawing 3 . Drawing 2 expresses the screen which picturized the eyegrounds image using the television camera, and shows notionally the result made binary so that suitable pretreatment might be performed and the blood vessel section 201 might become black. The code train generation section 103 searches for the point 202 which is equivalent to a mammary-papilla core from the blood vessel pattern 201 first from this image. Next, it asks for all intersections (204 white round heads) with a blood vessel pattern supposing the circle (dotted line shown by 203) of the radius beforehand decided considering the point 202 as a center.
[0019] Drawing 3 extracted and showed the circle 203 and the intersection 204. As shown in drawing 3 , two or more intersections 204 (they may be seven pieces by a diagram) can divide a circle 203 into two or more circles, and each arc chord angles T1-T7 can be determined. Then, the code train generation section 103 shown in drawing 1 generates code train information with reference to these angles T1-T7. for example, T -- 1= 109 T 2= 40 degrees, T3=32 degree, and T-four= -- T 5= 54 degrees, T 6= 62 degrees, supposing it is T 7= 38 degrees, each can be arranged in order as an integer of triple figures 25 degrees, and the following decimal numbers of 21 figures can be made into the code train C.
[0020]
C=1090400320250540620 38 -- (1)
The acquired code train C is used as a "private key" for carrying out the electronic signature of the document so that it may mention later. However, of course, it is also possible to use other

codes decided not based on code train C itself but based on the code train C as a "private key." Usually, since it is premised on using the prime factor as a "private key" and a "public key" in an unsymmetrical public key system, it may ask for the prime factor nearest to the value of the code train (1) instead of the code train (1) itself, it can be placed and treated in the code train C, and you may use as a private key.

[0021] The code train C is changed into secondary code information S in the secondary code information generation section 104 shown in drawing 1 below. Although various methods of searching for secondary code information S from the code train C are considered, it is effective to perform conversion using the following special functions F called a tropism function on the other hand. On the other hand, a tropism function is y, i.e., y=F, about x and an output in the input of Function F (x). -- (2)

Although asking for x to y is easy when it carries out, y is given and a function which is very difficult asks reverse for x. The case where consider as such a function, for example, repeat activation of the conversion by the following nonlinear functions G is carried out can be considered.

[0022]

y=G(x) =4x(1-x)2 -- (3)

That is, let the code train C generated by 103 be initial value x0. Here, although the code train C is the integer of 21 figures as shown in (1), since x of (3) types is the real number of 0 to 1, it shall use the value which did the division of the code train (1) by 1000000000000000000 000 as x0, and was changed into the real number value of 0-1.

[0023] This x0 is substituted for x of (3) types, and it asks for an output y0. namely, -- y0=G(x0) =4(x0) (1-x0) 2 -- (4)

The conversion same as xone is performed for y0 obtained next, and y1 is obtained. namely, -- x1=y0 y1=G(x1) =4(x1) (1-x1) 2 -- (5)

It asks for y2=G (x2) by making y1 obtained into x2, and for example, 100 circuit ****** and y100 are obtained in the same procedure like ..

[0024] In the secondary code information generation section 104, these y100 will be set up as secondary code information S. Namely, S=y100=F (C) -- (6)

Although Function F is a 100 circuit ********** function about G, and it is easy like the above explanation to search for secondary code information S from the code train C since it has the property of a tropism function on the other hand if it writes, it is impossible to ask reverse for the code train C from secondary code information S as a matter of fact.

[0025] Although secondary code information S is searched for in the above procedure, the owner A of a private key has performed the same thing beforehand using his biological information, a private key C and secondary code information S are searched for, and the secondary code information storage section which sets secondary acquired code information S to S0, and is shown by 105 is made to memorize beforehand in the example of a gestalt of this operation. Moreover, coincidence can be asked for the "public key" corresponding to a "private key" C at this time. Moreover, how to generate a "private key" and a "public key" using C is also considered, not using C itself as a "private key." For example, if the value of C is calculated, it can ask for the maximum prime factor P smaller than it and the minimum larger prime factor Q than it, and it can also constitute so that a "private key" and a "public key" may be generated by the well-known methods, such as a RSA method, using P and Q.

[0026] Since S0 memorized by the secondary code information storage section 105 cannot perform counting the code train C backward from S0 as a matter of fact even if it is stolen by others, a "private key" C is not known by others. moreover, S0 is good also as a configuration into which S0 is made to input as a symbol string each time from the user interface section which may record on other locations and is not a drawing example in that case.

[0027] The justification check section 106 checks whether secondary code information S0 beforehand memorized by the secondary code information storage section 105 and secondary code information S by which current generation is carried out are the same. This should just judge whether S and S0 are only equal. If S and S0 are equal, the biological information which made secondary code information S generate is equal to Mr. A's thing, i.e., it will be checked that

those who are going to do the electronic signature by the private key now using this system are [Mr. / itself / A].
[0028] This justification check section 106 will send the private key authorization flag En to the encryption section 108, if justification is checked. The encryption section 108 checks what the private key authorization flag En is outputted for (it is effective), uses the living body code C as a "private key" for the document data 107 (document information D inputted) shown by 107, performs encryption processing, and generates the encryption document (it is written as E (D, C)) shown in 109.
[0029] Since the encryption data 109 is decipherable with Mr. A's "public key", it becomes the same thing and it can be considered that it is Mr. A's signature document as Mr. A "signed." The above actuation is guaranteed because it has the feature which eyegrounds blood vessel patterns completely differ for every individual, and is referred to as eternal throughout life in an individual. That is, when the code train generated above was the same person, it turned into the always same code train, and it is based on the feature that an always different code train to others is generable.
[0030] although the voiceprint contained in the fingerprint pattern and voice other than an eyegrounds blood vessel pattern, the gene sequence included in DNA have the hand information when writing an alphabetic character etc. as such a living body feature, if the stability of code train generation is securable, and the same code train is always generable to the same individual namely,, of course, which biological information may be used
[0031] As explained above, risk of according to the example of a gestalt of this operation, being able to raise the reliability of the electronic signature using an individual private key, and the private key being referred to as being abused for others is beforehand avoidable.
Although the case where it was said that the code train which carried out the [example of gestalt of the second operation] above and which is generated from biological information in the example of a gestalt of the first operation can generate a code train which will turn into the always same code train if it is the same person, and is always different to others was explained, this invention is not limited to the above example. The example of a gestalt of implementation of the second invention concerning this invention which can be applied when a different code train to the same person may be generated is explained using drawing 4 .
[0032] Also in the example of a gestalt of the second operation, although the fundamental configuration is the same as that of drawing 1 , when [which is shown in drawing 4] justification is not checked in the justification check section 106, it controls to make each processing of the biological information acquisition in each configuration of the biological information acquisition section 101, the feature-extraction section 102, and the code train generation section 103, a feature extraction, and code train generation rerun, as an arrow head shows in the case of the example of a gestalt of the second operation,.
[0033] this is always stabilized and biological information can acquire it — not restricting — even if — a candidate — the owner of a private key — it is because the code train C acquired may shift delicately even if it is him. Therefore, it performs repeating re-acquisition until it performs repicturizing after it makes it make it picturize after shifting a little a candidate's eyeball location to image pick-up equipment as opposed to the biological information acquisition section 101, in acquiring an eyegrounds image, or tuning the brightness of the light source for illuminating eyegrounds finely and a delicate gap of a code train is solved.
[0034] It is not limited when surely performing re-acquisition control from acquisition of the biological information by the biological information acquisition section 101, and you may make the processing after the feature-extraction processing by the feature-extraction section 102 rerun, or code train generation processing of the code train generation section 103 may be made to rerun. What is necessary is just to control to judge whether generation of a code train is wound and ****(ed) and a justification check can be performed, changing the threshold of binary-izing when carrying out a feature extraction from an eyegrounds image to several steps in this case, or changing precision of the angle decision of a blood vessel.
[0035] If S0 and a match appear as S generated from the code train C in such two or more trial, a justification check will be materialized there and subsequent processings will be continued like

the example of a gestalt of the first operation. the case where specify the count of such retry beforehand and this count is exceeded -- a candidate -- a private key owner -- what is necessary is to conclude that he is not him and just to end signature processing
[0036] Also in the example of a gestalt of the above operation, the voiceprint contained in the fingerprint pattern and voice other than an eyegrounds blood vessel pattern, the gene sequence included in DNA can absorb it, even if it is available and the unstable factor is included to some extent in the feature extraction in the hand information when writing an alphabetic character etc. As explained above, when a different code train to the same person may be generated in the example of a gestalt of the second operation, the reliability of the electronic signature using an individual private key can be raised, and risk of the private key being referred to as being abused for others can be avoided beforehand.
[0037] In addition, although the example of a gestalt of the first which more than explained, and the second operation explained the case where an object document was enciphered using Mr. A's private key (signature), naturally of course, it can apply as it is also about the reverse. That is, it is the case where it is said that the document with which the document was enciphered using Mr. A's public key, and delivery and Mr. A have been seen off in Mr. A is decoded using its own private key other than [someone of] Mr. [A] Since the document enciphered with Mr. A's public key is decipherable with Mr. A's private key, it becomes an effective method to send a document so that it cannot decode only to Mr. A and cannot decode only to Mr. A in this way with the procedure of the example of a gestalt of the second operation, since a private key is generated from Mr. A's living body feature.
[0038] In such a case, it becomes the decode section in which the sent encryption document is equivalent to the document data 107 shown in drawing 1 , and the encryption section 108 decodes a document using a private key, and the encryption document data 109 will be equivalent to the document of the basis decoded and restored.
The case where the above function as an example of a gestalt of the third operation concerning [example of gestalt of the 3rd operation] this invention is applied to a reproducing unit is explained with reference to drawing 5 and drawing 6 . In the example of a gestalt of the third operation, the configuration in a manuscript copy system as shown in drawing 5 is explained. In drawing 5 , the same number is given to a configuration as well as the configuration of the example of a gestalt of the first operation shown in drawing 1 mentioned above, and details explanation is omitted.
[0039] Among drawing 5 , although it reaches and 108 is the same as that of drawing 1 , the document (manuscript document) 401 written to data medium, such as paper, is considered as 101-106, and a document that should sign in the example of a gestalt of the third operation. Moreover, 402 is the manuscript reading section which carries out scanning optically etc., reads this manuscript document, and changes it into a corresponding digital signal, 403 is the output section which changes the encryption data from the encryption section 108 into corresponding visible image information, for example, carries out a printout, and 404 is an encryption visible image (encryption document) outputted from the output section 403.
[0040] Usually, in the manuscript reproducing unit of a digital method, the manuscript document 401 is changed into the electrical signal for every pixel by the well-known manuscript reader 402, and various processings are performed to it as a digital picture signal, and it outputs the copy image of a manuscript document from the output section 403 represented with a laser beam type electrostatic printing method (for example, printout). In the example of a gestalt of the third operation, the manuscript image 401 is read by the manuscript read station 402. And the manuscript picture signal D read using the "private key" information C acquired in the procedure which was mentioned above in the encryption section 108, and which was explained in the example of a gestalt of the first operation is enciphered by the well-known method, and the enciphered picture signal E (D, C) is outputted to the output section 403.
[0041] In the output section 403, this encryption data is changed into corresponding visible image information, for example, it outputs on a record medium as an encryption document image 404. namely, the encryption document 404 outputted -- not the copy image of a manuscript image but the enciphered contents -- it becomes unknown hard copy printed matter. Drawing 6

shows the configuration when decoding the encryption document outputted by the configuration of drawing 5 . The encryption document 404 is read by the same manuscript reading section 402 as the configuration shown in drawing 5 , and is disassembled into the electrical signal with which it corresponds for every pixel.
[0042] The "public key" information corresponding to the "private key" when on the other hand enciphering from the user interface section 406 which is not illustrated is inputted. In the decode section 405, it transmits to the output section 403 from the read encryption document image and "public key" information by making into a picture signal the result decoded by decoding an encryption image, and in the output section 403, it changes into a corresponding visible image and the output-statement document 407 is generated. If it corresponds to a private key when the inputted public key enciphers, the output-statement document 407 should become the same thing as the manuscript document 401. That is, it can decide that an output-statement document is a document (signed) enciphered by the owner (namely, Mr. A) of a private key.
[0043] the case where the inputted public key does not belong to Mr. A -- naturally -- the output-statement document 407 -- a manuscript document -- it cannot restore -- contents -- the case where Mr. A does not encipher even if the unknown output was only carried out and the public key belonged to Mr. A (that is, not enciphered with Mr. A's private key) -- the same -- contents -- an unknown document will be outputted. Although considered as the configuration which uses Mr. A's public key for decoding and outputting an encryption document here, this is because the unsymmetrical public-key-encryption-ized method is used, and it is also possible to use other cipher systems.
[0044] For example, since the same cryptographic key as the both sides of encryption and decode is used when the usual object key cipher system is used, what is necessary will be just to use for this the private key which gave [above-mentioned] explanation. That is, encryption of a manuscript document is performed like the above-mentioned procedure, performs private key generation by the living body feature extraction also at the time of decode, and decodes an encryption document. in such a case -- the configuration that only he (Mr. A) who enciphered the manuscript document can do decode of an encryption document -- it can carry out -- him -- the information which be not known to except can be safely kept in the form of an encryption document.
[0045] In addition, although the above explanation outputted encryption information on the end record medium, the output in this output section 403 may be the digital data with which it is not limited in the case of the printout to the recording paper etc., and a record output may be carried out at the record medium of large capacity storage like a magnetic disk drive as digital data, for example, the encryption document 404 was memorized by this record medium, and may be document data with which the printout of the output-statement document 407 was carried out to paper etc. In this case, in order to decode the encryption digital data memorized, the manuscript reading section 402 is unnecessary and data is sent to the direct decode section 405.
[0046] Furthermore, the output of the output section 403 is not limited to a printout, even if the display output of it is carried out to an indicating equipment, it is stopped, and you may make it record digital data on other record media.
[0047]
[Other operation gestalten] In addition, even if it applies this invention to the system which consists of two or more devices (for example, a host computer, an interface device, a reader, a printer, etc.), it may be applied to the equipments (for example, a copying machine, facsimile apparatus, etc.) which consist of one device. Moreover, it cannot be overemphasized by the purpose of this invention supplying the storage which recorded the program code of the software which realizes the function of the operation gestalt mentioned above to a system or equipment, and reading and performing the program code with which the computer (or CPU and MPU) of the system or equipment was stored in the storage that it is attained.
[0048] In this case, the function of the operation gestalt which the program code itself by which reading appearance was carried out from the storage mentioned above will be realized, and the storage which memorized that program code will constitute this invention. As a storage for

supplying a program code, a floppy disk, a hard disk, an optical disk, a magneto-optic disk, CD-ROM, CD-R, a magnetic tape, the memory card of a non-volatile, ROM, etc. can be used, for example.

[0049] Moreover, it cannot be overemphasized that it is contained also when the function of the operation gestalt which performed a part or all of processing that OS (operating system) which is working on a computer is actual, based on directions of the program code, and the function of the operation gestalt mentioned above by performing the program code which the computer read is not only realized, but was mentioned above by the processing is realized.

[0050] Furthermore, after the program code by which reading appearance was carried out from a storage is written in the memory with which the functional expansion unit connected to the functional add-in board inserted in the computer or a computer is equipped, it is needless to say in being contained also when the function of the operation gestalt which performed a part or all of processing that CPU with which the functional add-in board and functional expansion unit are equipped based on directions of the program code is actual, and mentioned above by the processing is realized.

[0051] When applying this invention to the above-mentioned storage, the program code which realizes the function explained previously will be stored in the storage.

[0052]

[Effect of the Invention] As explained above, risk of according to this invention, being able to raise the reliability of the electronic signature using an individual private key, and the private key being referred to as being abused for others is beforehand avoidable.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is a block diagram explaining the example of a gestalt of implementation of the first invention concerning this invention.
[Drawing 2] **
[Drawing 3] It is drawing explaining an example of the living body feature extraction used for the example of a gestalt of this operation.
[Drawing 4] It is a block diagram explaining the example of a gestalt of implementation of the second invention concerning this invention.
[Drawing 5] **
[Drawing 6] It is a block diagram explaining the example of a gestalt of implementation of the third invention concerning this invention.
[Description of Notations]
101 Biological Information Acquisition Section
102 Feature-Extraction Section
103 Code Train Generation Section
104 Secondary Code Information Generation Section
105 Secondary Code Information Storage Section
106 Justification Check Section
108 Encryption Section
201 Blood Vessel Pattern
202 Point equivalent to Mammary-Papilla Core
204 Intersection of Circle 203 and Blood Vessel Pattern
402 Manuscript Reading Section
403 Output Section
405 Decode Section
406 User Interface Section

[Translation done.]

(C)

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－215119

(43)公開日　平成11年(1999)８月６日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３Ｄ
Ａ６１Ｂ	5/117		Ｇ０９Ｃ	1/00	６２０Ｂ
Ｇ０６Ｔ	7/00				６３０Ｚ
Ｇ０９Ｃ	1/00	６２０			６４０Ｂ
		６３０	Ａ６１Ｂ	5/10	３２０Ａ

審査請求　未請求　請求項の数14　ＯＬ　（全９頁）　最終頁に続く

(21)出願番号　特願平10－11764

(22)出願日　平成10年(1998)１月23日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　太田　健一
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

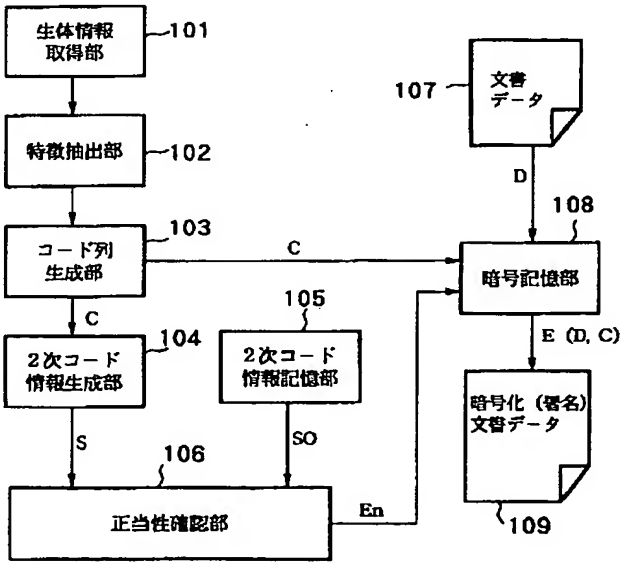
(74)代理人　弁理士　大塚　康徳　（外２名）

(54)【発明の名称】　個人情報管理装置及び方法

(57)【要約】

【課題】　個人の秘密鍵を用いた電子署名の信頼性を向上させると共に、その秘密鍵を他人に悪用されるという危険を未然に回避する。

【解決手段】　特徴抽出部１０２は、生体情報収得部１０１で収得した個人の生体情報（例えば眼底カメラ撮影画像）より生体特徴を抽出し、コード列生成部１０３は抽出された生体特徴をデジタルコード化してコード列Ｃを生成する。２次コード情報生成部１０４はこのコード列Ｃにもとづいて２次コード情報Ｓを生成する。正当性確認部１０６は、２次コード情報Ｓと予め登録されていた２次コード情報Ｓ０とを比較して特定個人よりの収得情報であると確認すると文書データを暗号化部１０８で前記生成したコード列Ｃを用いて暗号化して署名データ１０９を生成する。



【特許請求の範囲】

【請求項１】　個人の生体特徴を抽出する抽出手段と、前記抽出手段で抽出された生体特徴をデジタルコード化するコード化手段と、

前記コード化手段でコード化されたデジタルコードにもとづいて２次コード情報を生成する２次コード生成手段と、

前記生成手段で生成された２次コード情報の正当性を確認する確認手段と、

前記確認手段で正当性が確認された場合に前記コード化手段でコード化された生体特徴に基づいて署名データを生成する署名データ生成手段とを有することを特徴とする個人情報管理装置。

【請求項２】　前記署名データ生成手段は、前記確認手段で正当性が確認されない場合に、前記抽出手段による個人の生体特徴の抽出、及び前記コード化手段による生体特徴のデジタルコード化処理をやり直させることを特徴とする請求項１記載の個人情報管理装置。

【請求項３】　前記署名データ生成手段は、処理対象データを前記コード化手段でコード化された生体特徴に基づいて暗号化して暗号化データを署名データとすることを特徴とする請求項１又は請求項２のいずれかに記載の個人情報管理装置。

【請求項４】　原稿画像を読み取り、原稿画像信号として出力可能な原稿画像読み取り手段と、前記原稿画像読み取り手段で読み取られた原稿画像信号を対応する可視画像として出力する出力手段とを有する原稿画像複写システムに組み込み可能な個人情報管理装置であって、

個人の生体特徴を抽出する抽出手段と、

前記抽出手段で抽出された生体特徴をデジタルコード化するコード化手段と、

前記コード化手段でコード化されたデジタルコードにもとづいて２次コード情報を生成する２次コード生成手段と、

前記生成手段で生成された２次コード情報の正当性を確認する確認手段と、

前記確認手段で正当性が確認された場合に前記コード化手段でコード化された生体特徴に基づいて前記原稿画像読み取り手段で読み取られた原稿画像信号を暗号化する暗号化手段と、

前記暗号化手段で暗号化された信号を可視画像データに変換して前記出力手段に出力する変換手段とを有することを特徴とする個人情報管理装置。

【請求項５】　前記２次コード情報は生体特徴をデジタルコード化したコード列を所定の一方向性関数によって変換して生成するものであることを特徴とする請求項１乃至請求項４のいずれかに記載の個人情報管理装置。

【請求項６】　前記２次コード情報の正当性は、予め登録されている２次コード情報と前記２次コード生成手段で生成された２次コード情報との比較によって確認されることを特徴とする請求項１乃至請求項５のいずれかに記載の個人情報管理装置。

【請求項７】　個人の生体特徴を抽出して抽出した生体特徴をデジタルコード化し、前記コード化されたデジタルコードにもとづいて２次コード情報を生成して生成した２次コード情報の正当性を確認し、正当性が確認された場合に前記コード化された生体特徴に基づいて署名データを生成する署名データ生成することを特徴とする個人情報管理方法。

【請求項８】　前記２次コード情報の正当性が確認されない場合には前記個人の生体特徴の抽出、及び前記生体特徴のデジタルコード化処理をやり直させることを特徴とする請求項７記載の個人情報管理方法。

【請求項９】　前記署名データの生成は、処理対象データを前記コード化手段でコード化された生体特徴に基づいて暗号化して暗号化データを署名データとするものであることを特徴とする請求項７又は請求項８のいずれかに記載の個人情報管理方法。

【請求項１０】　原稿画像を読み取り、原稿画像信号として出力可能な原稿画像読み取り手段と、前記原稿画像読み取り手段で読み取られた原稿画像信号を対応する可視画像として出力する出力手段とを有する原稿画像複写装置における個人情報管理方法であって、

個人の生体特徴を抽出して抽出された生体特徴をデジタルコード化し、前記コード化されたデジタルコードにもとづいて２次コード情報を生成して生成された２次コード情報の正当性を確認し、正当性が確認された場合に前記コード化された生体特徴に基づいて前記原稿画像読み取り手段で読み取られた原稿画像信号を暗号化し、更に暗号化された信号を可視画像データに変換して前記出力手段に出力することを特徴とする個人情報管理方法。

【請求項１１】　前記２次コード情報は生体特徴をデジタルコード化したコード列を所定の一方向性関数によって変換して生成するものであることを特徴とする請求項７乃至請求項１０のいずれかに記載の個人情報管理装置。

【請求項１２】　前記２次コード情報の正当性は、予め登録されている２次コード情報と前記２次コード生成手段で生成された２次コード情報との比較によって確認されることを特徴とする請求項７乃至請求項１１のいずれかに記載の個人情報管理方法。

【請求項１３】　請求項1乃至請求項１２のいずれかに記載の機能を実現する制御手順を記録してなることを特徴とするコンピュータ可読記録媒体。

【請求項１４】　請求項1乃至請求項１２のいずれかに記載の機能を実現することを特徴とするコンピュータプログラム列。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は個人の生体的特徴に

基づいて個人情報を管理し、例えば個人の生体的特徴に基づいて個人の署名情報や原稿複写を制御可能な個人情報管理装置及び方法に関するものである。

【０００２】

【従来の技術】現在、ネットワークシステムが発展し、ネットワーク上での電子決済や電子マネーといった技術が数多く検討されている。このネットワークシステムを利用して個人が電子的に取引きを行おうとする場合、取引を要求している個人を遠隔地から正確に識別しなければならない。このため、ＲＳＡ方式などのいわゆる非対称公開鍵方式を利用した電子署名技術が検討されている。

【０００３】非対称公開鍵方式は「公開鍵」と「秘密鍵」という一対の鍵情報を設定し、個人が持っている秘密鍵を用いて個人の発行する文書に署名しておくと、同一人の公開鍵によらなければその文書を解読できないという特徴がある。そこで、個人（Ａさんとする）が秘密鍵を絶対に他人に知られないように管理し、Ａさんが取り引きの発注文書をその秘密鍵で暗号化して取り引き相手（Ｂさんとする）に送信すれば、Ｂさんはその文書がＡさんの公開鍵でしか解読できないので注文書の発行者が間違いなくＡさんである、ということが確認できる。

【０００４】一方、特定個人をより正確に認証するために、眼底カメラ等の眼科装置により、エリアＣＣＤ等の固体撮像素子を用いて眼底像を電子撮影し、電子撮像した映像信号をハードディスク等の記憶媒体に記憶し、この記憶媒体に記憶された過去の眼底像と、新たに電子撮影された現在の眼底像とを比較して個人を識別するようにした個人識別装置が知られている。

【０００５】

【発明が解決しようとする課題】しかし、上記従来例の暗号化システムにおいては、以下の様な問題点があった。即ち、上述したような一般的な非対称公開鍵方式を利用した電子署名技術においては、個人を識別するために秘密鍵と呼ばれるパスワードを設定する必要があるが、他人による鍵の盗用を防ぐためにはある程度複雑なパスワードにしなければならず、確実なものとするにはその桁数なども多くしなければならず、個人の記憶できる限界を越えてしまい実用的でないという問題がある。

【０００６】このパスワードを個人で記憶しておくのではなく何らかの記憶装置上に記憶させて保存しておくという方法も考えられるが、その記憶装置が他者から読み出されないという保証は無く、安全性という観点で問題がある。また、眼底像を用いて個人認証しようという場合、個人を特定するための情報、すなわち個人の眼底像を電子撮影した画像情報をあらかじめ記憶装置に記憶しておかねばならず、この記憶情報が盗用されてしまった場合には信頼性の高い個人認証が不可能になってしまう、という問題があった。

【０００７】以上のように、電子的取引における個人認証の問題を解決するような有効な方法は提案されていなかった。

【０００８】

【課題を解決するための手段】本発明は上述した課題を解決することを目的としてなされたもので、かかる目的を達成する一手段として例えば以下の構成を備える。即ち、個人の生体特徴を抽出する抽出手段と、前記抽出手段で抽出された生体特徴をデジタルコード化するコード化手段と、前記コード化手段でコード化されたデジタルコードにもとづいて２次コード情報を生成する２次コード生成手段と、前記生成手段で生成された２次コード情報の正当性を確認する確認手段と、前記確認手段で正当性が確認された場合に前記コード化手段でコード化された生体特徴に基づいて署名データを生成する署名データ生成手段とを有することを特徴とする。

【０００９】そして例えば、前記署名データ生成手段は、前記確認手段で正当性が確認されない場合に、前記抽出手段による個人の生体特徴の抽出、及び前記コード化手段による生体特徴のデジタルコード化処理をやり直させることを特徴とする。又例えば、前記署名データ生成手段は、処理対象データを前記コード化手段でコード化された生体特徴に基づいて暗号化して暗号化データを署名データとすることを特徴とする。

【００１０】または、原稿画像を読み取り、原稿画像信号として出力可能な原稿画像読み取り手段と、前記原稿画像読み取り手段で読み取られた原稿画像信号を対応する可視画像として出力する出力手段とを有する原稿画像複写システムに組み込み可能な個人情報管理装置であって、個人の生体特徴を抽出する抽出手段と、前記抽出手段で抽出された生体特徴をデジタルコード化するコード化手段と、前記コード化手段でコード化されたデジタルコードにもとづいて２次コード情報を生成する２次コード生成手段と、前記生成手段で生成された２次コード情報の正当性を確認する確認手段と、前記確認手段で正当性が確認された場合に前記コード化手段でコード化された生体特徴に基づいて前記原稿画像読み取り手段で読み取られた原稿画像信号を暗号化する暗号化手段と、前記暗号化手段で暗号化された信号を可視画像データに変換して前記出力手段に出力する変換手段とを有することを特徴とする。

【００１１】そして例えば、前記２次コード情報は生体特徴をデジタルコード化したコード列を所定の一方向性関数によって変換して生成するものであることを特徴とする。又例えば、前記２次コード情報の正当性は、予め登録されている２次コード情報と前記２次コード生成手段で生成された２次コード情報との比較によって確認されることを特徴とする。又、個人の生体特徴を抽出して抽出した生体特徴をデジタルコード化し、前記コード化されたデジタルコードにもとづいて２次コード情報を生成して生成した２次コード情報の正当性を確認し、正当

性が確認された場合に前記コード化された生体特徴に基づいて署名データを生成する署名データ生成する手段を有することを特徴とする。

【００１２】

【発明の実施の形態】以下、図面を用いて本発明に係る一発明の実施の形態例について詳細に説明する。

［第一の実施の形態例］以下、本発明に係る第一の発明の実施の形態例を説明する。第一の発明の実施の形態例では、ある個人（Ａさんとする）がＲＳＡ方式などの非対称公開鍵暗号システムを利用して、対象となる文書データに、本実施の形態例の電子署名を行なう場合を想定して説明する。

【００１３】通常、非対称公開鍵暗号システムではＡさんは２つの暗号鍵として「秘密鍵」と「公開鍵」を所有している。いずれも数十ビットから数百ビットのビット列で表現されており「秘密鍵」はＡさんしか知らないが「公開鍵」は一般に公開されているものである。今、ある文書をＡさんが自分の「秘密鍵」を用いて暗号化した場合、暗号化された文書はＡさんの公開鍵によらなければ解読することができない。

【００１４】Ａさんの「秘密鍵」はＡさん以外には知られていないので、ある文書がＡさんの「公開鍵」で解読できるということは、その文書がＡさんによって暗号化された、すなわちＡさん本人が署名した文書である、ということが確定される。しかし、以上において「秘密鍵」が本人以外に知られていないということが前提であるので、これを厳重に保管しておく必要があるが従来例で説明したとおり、個人が記憶しておいたり、あるいはなんらかのデジタルデータとして記憶媒体に記憶させておかなければならず、その安全性は十分ではない。

【００１５】本実施の形態例では図１の構成を用いることにより「秘密鍵」の安全性を保証することができる。図１は本発明に係る第一の発明の実施の形態例における個人情報管理装置の構成を示すブロック図である。図１において、１０１は生体情報収得部であり、秘密鍵を所有している個人（ここではＡさん）の生体情報の取得を行う。例えばＣＣＤ撮像素子を用いた眼底カメラによって眼底の網膜血管パターンを撮像したり、あるいは指紋パターン像を２次元的に取得したりといった、特定個人を同定するために有効であると言われている生体的な情報を周知の方法で取得する。

【００１６】１０２は特徴抽出部であり、特徴抽出部１０２は、生体情報収得部１０１で得られた生体情報から特徴抽出を行う。例えば眼底の血管パターンから特徴量を抽出する方法としては特開平７－２１３５１１号（「個人識別装置」）に示されているようなものを用いることができる。これは眼底像から乳頭中心位置を検出し、その中心位置から同心円状に眼底像を走査して血管の存在する位置の角度成分を検出するものである。

【００１７】１０３はコード列生成部であり、特徴抽出部１０２で抽出した生体情報の特徴から得られた角成分をもとにして所定のコード列を生成する。例えば、上述した特開平７－２１３５１１号では検出された角度成分をあらかじめ保存してある特定個人の参照パターンと比較し、本人であるか否かを検出しているが、本実施の形態例では得られた角度成分をもとにしてコード列生成部１０３により所定のコード列を生成する。

【００１８】図２及び図３にコード列生成部１０３によるコード列生成の様子を示す。図２は眼底像をテレビカメラを用いて撮像した画面を表しており、適当な前処理を行って血管部２０１が黒くなるように２値化した結果を概念的に示したものである。コード列生成部１０３は、この画像に対し、まず血管パターン２０１から乳頭中心部に相当する点２０２を求める。次に点２０２を中心としてあらかじめ決められた半径の円（２０３で示される点線）を想定し、血管パターンとの交点（２０４の白丸）を全て求める。

【００１９】円２０３と交点２０４を抜き出して示したのが図３である。図３に示すように複数の交点２０４（図では７個としてある）が円２０３を複数の円弧に分割し、各々の円弧の角度Ｔ１～Ｔ７を決定することができる。そこで図１に示すコード列生成部１０３は、この角度Ｔ１～Ｔ７を参照してコード列情報を生成する。例えばＴ１＝１０９度、Ｔ２＝４０度、Ｔ３＝３２度、Ｔ４＝２５度、Ｔ５＝５４度、Ｔ６＝６２度、Ｔ７＝３８度であったとするとそれぞれを３桁の整数として順番に並べて次のような２１桁の１０進数をコード列Ｃとすることができる。

【００２０】

Ｃ＝１０９０４００３２０２５０５４０６２０３８　　…（１）

得られたコード列Ｃは後述するように文書を電子署名するための「秘密鍵」として使用する。ただし、コード列Ｃそのものではなくコード列Ｃに基づいて決められる他のコードを「秘密鍵」として用いることももちろん可能である。通常非対称公開鍵方式では「秘密鍵」や「公開鍵」として素数を使用することを前提としているので、コード列（１）そのものではなくコード列（１）の値に最も近い素数を求め、それをコード列Ｃに置き換えて秘密鍵として用いてもよい。

【００２１】コード列Ｃは次に図１に示す２次コード情報生成部１０４で２次コード情報Ｓに変換される。コード列Ｃから２次コード情報Ｓを求める方法は種々考えられるが、以下のような一方向性関数と呼ばれる特殊な関数Ｆを用いた変換を行うのが効果的である。一方向性関数とは、関数Ｆの入力をｘ、出力をｙ、すなわち

ｙ＝Ｆ（ｘ）　　…（２）

とした場合、ｘからｙを求めるのは容易だが、ｙを与えて、逆にｘを求めるのは非常に困難であるような関数の

ことである。このような関数として、例えば次のような非線形の関数Ｇによる変換を繰り返し実行する場合を考えることができる。

【００２２】

$$y=G(x)=4x(1-x)^2 \quad \cdots(3)$$

すなわち１０３で生成されたコード列Ｃを初期値ｘ０とする。ここで、コード列Ｃは（１）に示すような２１桁の整数であるが（３）式のｘは０から１の実数なのでｘ０としてはコード列（１）を１０００００００００００００００００００で除算して０～１の実数値に変換した値を用いるものとする。

$$y0=G(x0)=4(x0)(1-x0)^2 \quad \cdots(4)$$

つぎに得られたｙ０をｘ１として同じ変換を行いｙ１を

$$x1=y0$$

$$y1=G(x1)=4(x1)(1-x1)^2 \quad \cdots(5)$$

得られたｙ１をｘ２としてｙ２＝Ｇ（ｘ２）を求め、・・というように同じ手順を、例えば１００回線り返すとｙ１００が得られる。

【００２３】このｘ０を（３）式のｘに代入して出力ｙ０を求める。すなわち

得る。すなわち

等しい、すなわち現在このシステムを用いて秘密鍵による電子署名をしようとしている人がＡさんそのものであるということが確認される。

【００２４】２次コード情報生成部１０４では、このｙ１００を２次コード情報Ｓとして設定することにする。すなわち

$$S=y100=F(C) \quad \cdots(6)$$

と書くと、関数ＦはＧを１００回線り返して得られる関数であり、一方向性関数の性質を持つため、コード列Ｃから２次コード情報Ｓを求めるのは以上の説明のように容易であるが、２次コード情報Ｓから逆にコード列Ｃを求めるのは事実上不可能である。

【００２５】本実施の形態例においては、以上の手順で２次コード情報Ｓを求めるのであるが、同じことを秘密鍵の所有者Ａさんは自分の生体情報を用いて予め行って秘密鍵Ｃと２次コード情報Ｓを求めておき、得られた２次コード情報ＳをＳ０として１０５で示される２次コード情報記憶部にあらかじめ記憶させておく。またこのときに「秘密鍵」Ｃに対応する「公開鍵」も同時に求めておくことができる。また、Ｃそのものを「秘密鍵」として用いるのではなく、Ｃを使って「秘密鍵」と「公開鍵」を生成する方法も考えられる。例えば、Ｃの値を求めたら、それより小さい最大の素数Ｐとそれより大きい最小の素数Ｑを求め、Ｐ，Ｑを用いてＲＳＡ方式など周知の方法で「秘密鍵」と「公開鍵」を生成するように構成することもできる。

【００２６】２次コード情報記憶部１０５に記憶されているＳ０は、たとえ他人に盗まれたとしてもＳ０からコード列Ｃを逆算することが事実上できないので「秘密鍵」Ｃが他人に知られることはない。またＳ０は他の場所に記録しておいてもよく、その場合は図示しないユーザーインターフェース部からＳ０を記号列としてその都度入力させるような構成としてもよい。

【００２７】正当性確認部１０６は、あらかじめ２次コード情報記憶部１０５に記憶されている２次コード情報Ｓ０と、現在生成されている２次コード情報Ｓとが同一であるか否かを確認する。これは単にＳとＳ０が等しいかどうかを判定すればよい。ＳとＳ０が等しければ、２次コード情報Ｓを生成させた生体情報がＡさんのものと

【００２８】この正当性確認部１０６は、正当性を確認すると秘密鍵許可フラグＥｎを暗号化部１０８に送る。暗号化部１０８は秘密鍵許可フラグＥｎが出力されている（有効である）ことを確認して、１０７で示される文書データ１０７（入力される文書情報Ｄ）を生体コードＣを「秘密鍵」として暗号化処理を実行し、１０９に示す暗号化文書（Ｅ（Ｄ，Ｃ）と書く）を生成する。

【００２９】暗号化データ１０９は、Ａさんの「公開鍵」でしか解読できないのでＡさんが「署名」したのと同じことになりＡさんの署名文書とみなすことができる。以上の動作が保証されるのは眼底血管パターンが個人ごとに全く異なっており、また一個人においては終生不変であると言う特徴をもっているからである。つまり上記で生成されるコード列は同一人物であれば常に同じコード列となり、他人に対しては常に異なるコード列を生成できるという特徴によっている。

【００３０】このような生体特徴としては眼底血管パターンの他に指紋パターン、音声に含まれる声紋、ＤＮＡに含まれる遺伝子配列など、あるいは文字を書くときの筆跡情報などがあるが、コード列生成の安定性が確保できれば（すなわち、同一個人に対して常に同一のコード列を生成できれば）いずれの生体情報を利用しても良いことは勿論である。

【００３１】以上説明したように本実施の形態例によれば、個人の秘密鍵を用いた電子署名の信頼性を向上させることができ、またその秘密鍵を他人に悪用されるという危険を未然に回避することができる。

［第二の実施の形態例］前記した第一の実施の形態例において、生体情報から生成されるコード列は同一人物であれば常に同じコード列となり、他人に対しては常に異なるコード列を生成できるという場合について説明したが、本発明は以上の例に限定されるものではない。同一人物に対して異なるコード列が生成される可能性がある場合に適用可能な本発明に係る第二の発明の実施の形態例について図４を用いて説明する。

【００３２】図４に示す第二の実施の形態例において

も、基本的な構成は図１と同様であるが、第二の実施の形態例の場合は正当性確認部１０６で正当性が確認されなかった場合、矢印で示すように生体情報取得部１０１、特徴抽出部１０２、コード列生成部１０３の各構成における生体情報取得、特徴抽出、コード列生成の各処理を再実行させるように制御する。

【００３３】これは生体情報が常に安定して取得できるとは限らず、たとえ対象者が秘密鍵の所有者本人であったとしても得られるコード列Ｃが微妙にずれてしまう場合があるからである。そのため生体情報収得部１０１に対し、例えば眼底像を取得する場合には撮像装置に対する対象者の眼球位置を少しずらしてから撮像するようにさせたり、あるいは眼底を照明するための光源の明るさを微調整してから撮像し直す、といったことを行ってコード列の微妙なずれが解消するまで再取得を繰り返すといったことを行う。

【００３４】再取得制御は、必ず生体情報収得部１０１による生体情報の収得から行う場合に限定されるものではなく、特徴抽出部１０２による特徴抽出処理以降の処理を再実行させても、あるいは、コード列生成部１０３のコード列生成処理を再実行させるものであってもよい。この場合、例えば、眼底像から特徴抽出するときの２値化のしきい値を数段階に変化させたり、あるいは血管の角度決定の精度を変化させたりしながらコード列の生成を繰り返えして正当性確認ができるか否かを判断するように制御すればよい。

【００３５】このような複数の試行の中でコード列Ｃから生成されるＳとしてＳ０と一致するものが現れれば、そこで正当性確認が成立し、第一の実施の形態例と同様に以降の処理を継続する。このような再試行の回数はあらかじめ指定しておき、この回数を越えた場合、対象者は秘密鍵所有者本人ではないと断定して、署名処理を終了する様にすればよい。

【００３６】以上の実施の形態例においても、眼底血管パターンの他に、指紋パターン、音声に含まれる声紋、ＤＮＡに含まれる遺伝子配列など、あるいは文字を書くときの筆跡情報などを利用可能であり、またある程度特徴抽出に不安定な要因が含まれていてもそれを吸収することが可能である。以上説明したように第二の実施の形態例においては、同一人物に対して異なるコード列が生成される可能性がある場合においても、個人の秘密鍵を用いた電子署名の信頼性を向上させることができ、またその秘密鍵を他人に悪用されるという危険を未然に回避することができる。

【００３７】なお、以上の説明した第一及び第二の実施の形態例では、対象文書をＡさんの秘密鍵を用いて暗号化（署名）する場合について説明したが、当然その逆についてもそのまま適用可能であることは勿論である。すなわちＡさん以外の誰かがＡさんの公開鍵を用いて文書を暗号化してＡさんに送り、Ａさんが送られてきた文書を自分の秘密鍵を用いて解読する、という場合である。Ａさんの公開鍵で暗号化された文書はＡさんの秘密鍵でしか解読できないので、第二の実施の形態例の手順により、Ａさんの生体特徴から秘密鍵を生成するので、Ａさんだけにしか解読できず、このようにＡさんだけにしか解読できないように文書を送りたいときには有効な方法となる。

【００３８】このような場合、図１に示す文書データ１０７に相当するのが送られてきた暗号化文書であり、暗号化部１０８が秘密鍵を用いて文書を解読する解読部となり、暗号化文書データ１０９が解読され復元されたもとの文書に対応することになる。

［第３の実施の形態例］本発明に係る第三の実施の形態例として、以上の機能を複写装置に適用した場合を図５及び図６を参照して説明する。第三の実施の形態例においては、図５に示すような原稿複写システムにおける構成について説明する。図５において、上述した図１に示す第一の実施の形態例の構成と同様構成には同一番号を付して詳細説明を省略する。

【００３９】図５中、１０１～１０６、および１０８は図１と同様であるが、第三の実施の形態例においては署名すべき文書として、紙などの媒体に書かれた文書（原稿文書）４０１を考える。また、４０２はこの原稿文書を光学的に走査する等して読み取り、対応するデジタル信号に変換する原稿読み取り部であり、４０３は暗号化部１０８よりの暗号化データを対応する可視画像情報に変換して例えば印刷出力する出力部であり、４０４は出力部４０３より出力される暗号化可視画像（暗号化文書）である。

【００４０】通常、デジタル方式の原稿複写装置においては、原稿文書４０１は周知の原稿読み取り装置４０２によって画素毎の電気信号に変換され、デジタルの画像信号として各種処理を施され、レーザービーム式静電印刷方式で代表される出力部４０３から原稿文書の複写画像を出力（例えば印刷出力）するようになっている。第三の実施の形態例では、原稿画像４０１を原稿読取部４０２で読み取る。そして、暗号化部１０８で上述した第一の実施の形態例で説明した手順で得られた「秘密鍵」情報Ｃを用いて読み取られた原稿画像信号Ｄを周知の方法で暗号化し、暗号化された画像信号Ｅ（Ｄ，Ｃ）を出力部４０３に出力する。

【００４１】出力部４０３では、この暗号化データを対応する可視画像情報に変換して例えば暗号化文書画像４０４として記録媒体上に出力する。すなわち出力される暗号化文書４０４は、原稿画像の複写画像ではなく、暗号化された内容不明のハードコピー印刷物となる。図６は図５の構成により出力された暗号化文書を解読するときの構成を示す。暗号化文書４０４は、図５に示す構成と同様の原稿読み取り部４０２によって読み取られ、画素毎の対応する電気信号に分解される。

【００４２】一方、図示しないユーザーインターフェース部４０６から暗号化したときの「秘密鍵」に対応する「公開鍵」情報を入力する。解読部４０５では読み取られた暗号化文書画像と「公開鍵」情報から暗号化画像の解読を行い解読された結果を画像信号として出力部４０３へ転送し、出力部４０３では対応する可視画像に変換して出力文書４０７を生成する。　もし入力された公開鍵が暗号化したときの秘密鍵に対応するものであれば出力文書４０７は原稿文書４０１と同一なものとなるはずである。すなわち出力文書が秘密鍵の持ち主（すなわちＡさん）によって暗号化された（署名された）文書であるということが確定できる。

【００４３】入力された公開鍵がＡさんのものでない場合には当然出力文書４０７は原稿文書を復元できず、内容不明な出力がされるだけであり、また公開鍵がＡさんのものであっても暗号化を行ったのがＡさんではない（すなわちＡさんの秘密鍵で暗号化されていない）場合にも同様に内容不明な文書が出力されることになる。ここでは暗号化文書を解読して出力するのにＡさんの公開鍵を用いる構成としたが、これは非対称公開鍵暗号化方式を利用しているためであって、他の暗号化方式を用いることも可能である。

【００４４】例えば通常の対象鍵暗号方式を用いた場合は、暗号化、解読の双方に同じ暗号鍵を用いるので、上記説明した秘密鍵をこれに利用すればよいことになる。すなわち原稿文書の暗号化は上記手順と同様に行い、解読時にも生体特徴抽出による秘密鍵生成を行い暗号化文書の解読を行う。このような場合には原稿文書を暗号化した本人（Ａさん）のみしか暗号化文書の解読ができない、という構成とすることができ、本人以外に知られたくない情報を暗号化文書の形で安全に保管することができる。

【００４５】なお、以上の説明は暗号化情報を一端記録媒体上に出力したが、この出力部４０３での出力は記録紙等への印刷出力の場合に限定されるものではなく、例えばデジタルデータとして磁気ディスク装置の様な大容量記憶装置の記録媒体に記録出力されるものであってもよく、暗号化文書４０４がこの記録媒体に記憶されたデジタルデータで、出力文書４０７が紙などに印刷出力された文書データであってもよい。この場合、記憶されている暗号化デジタルデータを解読するために原稿読み取り部４０２は不要であり、データは直接解読部４０５へ送られる。

【００４６】更に、出力部４０３の出力は印刷出力に限定されるものではなく、表示装置に表示出力されるものであってもよし、また、他の記録媒体にデジタルデータを記録するようにしてもよい。

【００４７】

【他の実施形態】なお、本発明は、複数の機器（例えばホストコンピュータ，インタフェイス機器，リーダ，プリンタなど）から構成されるシステムに適用しても、一つの機器からなる装置（例えば、複写機，ファクシミリ装置など）に適用してもよい。また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。

【００４８】この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。プログラムコードを供給するための記憶媒体としては、例えば、フロッピディスク，ハードディスク，光ディスク，光磁気ディスク，ＣＤ－ＲＯＭ，ＣＤ－Ｒ，磁気テープ，不揮発性のメモリカード，ＲＯＭなどを用いることができる。

【００４９】また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているＯＳ（オペレーティングシステム）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００５０】さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００５１】本発明を上記記憶媒体に適用する場合、その記憶媒体には、先に説明した機能を実現するプログラムコードを格納することになる。

【００５２】

【発明の効果】以上に説明したように本発明によれば、個人の秘密鍵を用いた電子署名の信頼性を向上させることができ、またその秘密鍵を他人に悪用されるという危険を未然に回避することができる。

【図面の簡単な説明】

【図１】本発明に係る第一の発明の実施の形態例を説明するブロック図である。

【図２】、

【図３】本実施の形態例に利用される生体特徴抽出の一例を説明する図である。

【図４】本発明に係る第二の発明の実施の形態例を説明するブロック図である。

【図５】、

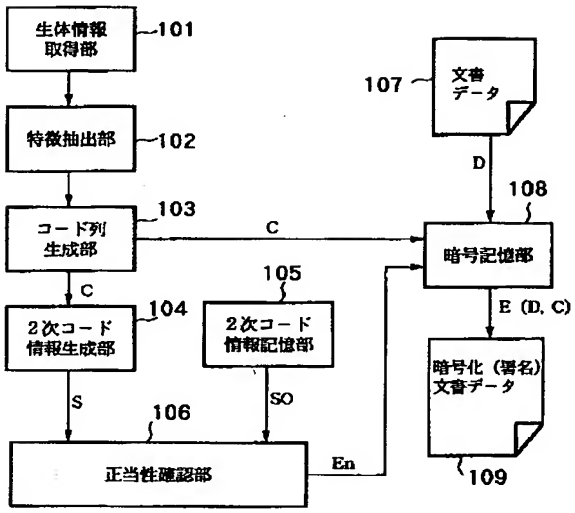
【図６】本発明に係る第三の発明の実施の形態例を説明

するブロック図である。

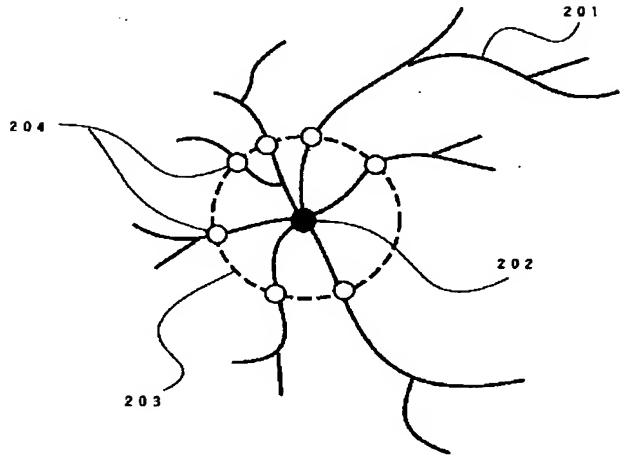
【符号の説明】

１０１　生体情報収得部
１０２　特徴抽出部
１０３　コード列生成部
１０４　２次コード情報生成部
１０５　２次コード情報記憶部
１０６　正当性確認部
１０８　暗号化部
２０１　血管パターン
２０２　乳頭中心部に相当する点
２０４　円２０３と血管パターンとの交点
４０２　原稿読み取り部
４０３　出力部
４０５　解読部
４０６　ユーザーインターフェース部

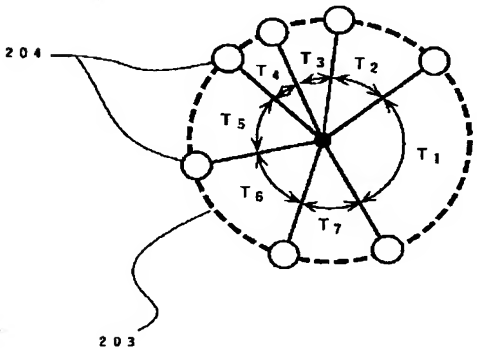
【図１】



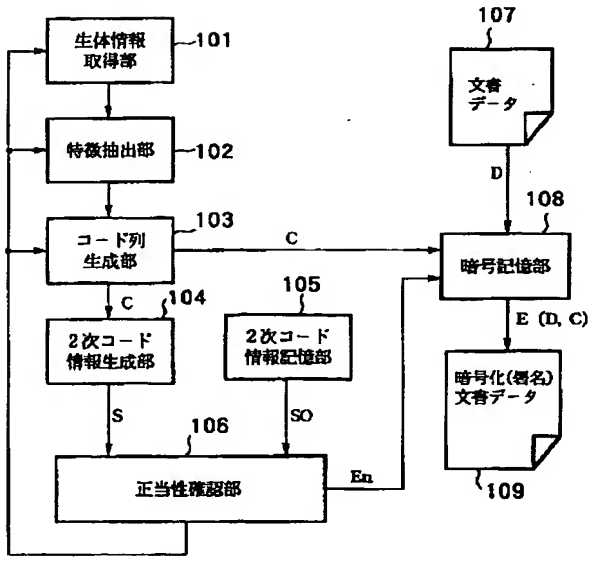
【図２】



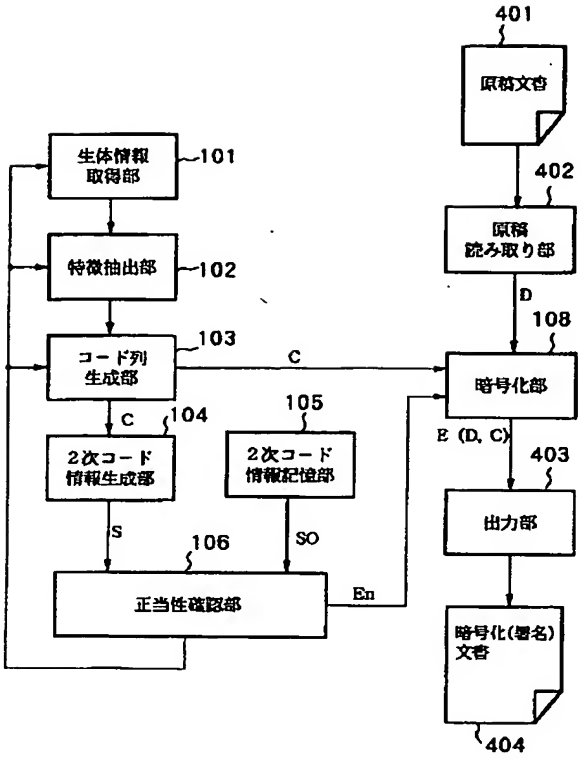
【図３】



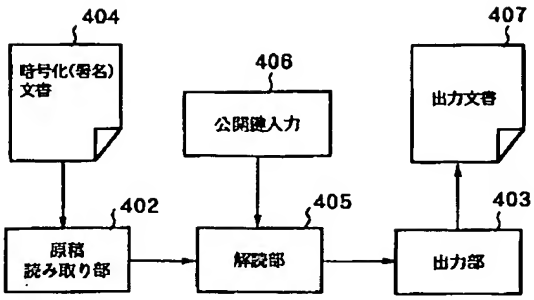
【図４】



【図５】



【図６】



フロントページの続き

(51)Int.Cl.[6]	識別記号	FI	
Ｇ０９Ｃ　1/00	６４０	Ｇ０６Ｆ　15/62	４６５Ｋ
		Ｈ０４Ｌ　9/00	６７５Ｂ